

Business Continuity Plan (BCP)

Policy Title	Business Continuity Plan (BCP)
Inception Date	28/02/2011
Reason for Review	Periodic review
Policy Owner	IT Manager / Representative
Approved By	VFM EXCO
Date approved: This version replaces all previous versions of the policy	01.08.2022

P O Box 44586, Claremont, 7735

1st Floor, 5 Cavendish Street, Claremont, 7708, Cape Town

T (021) 670 4900 | F (021) 683 5788 | E info@vunanifm.co.za | W www.vunanifm.co.za

Registration Number: 1999/015894/07. | Executive Directors: | Non-Executive Directors: N Chonco, E Dube

Vunani Fund Managers (Pty) Ltd is an authorised financial services provider. FSP License No.: 608

1) Emergency Contact Persons

Emergency contact persons are:

- a) iSquared – IT / System Support
support@isquared.co.za
021 671-5778
- b) Kirsten Elvin-Jensen – Chief Operating Officer
kirstenej@vunanifm.co.za
082-462-8090 (mobile)
021-789-2617 (home)
- c) Chantal Strydom – Relationship Manager / IT representative
chantals@vunanifm.co.za
082-413-4773 (mobile)
- d) Safs Narker – CIO
safsn@vunanifm.co.za
084-336-8013 (mobile)
- e) Craig MacArthur – Portfolio Manager
craigm@vunanifm.co.za
079-074-0471 (mobile)
021-712-2527 (home)

These names will be updated in the event of a material change, and the Executive Committee (EXCO) or its Representative will be responsible for updating.

2) Company Policy

VFM's Business Continuity Plan (BCP) seeks:

- a) to protect clients, employees, information, and assets until normal business operations are resumed.
- b) to ensure that a viable capability exists to respond to an incident and manage all responses and recovery activities including:
 - Data back-up and recovery
 - All mission critical systems

- Financial and operational assessments
 - Communications between the company and clients
 - Communications between the company and its employees and shareholders
 - Physical location of employees.
- c) to accomplish rapid and efficient resumption of critical business operations, technology, and functional support areas.
- d) to support and communicate with employees, regulatory agencies, and clients.
- e) to ensure all insurance and regulatory requirements are satisfied in the event of a crisis and activation of this Plan.

3) Scope of this Plan

This Plan covers:

- a) Significant Business Disruptions (SBDs):

This Plan addresses both internal and external SBDs.

- Internal SBDs only affect VFM's ability to communicate and do business, such as e.g., any event that denies access to the company's premises.
 - External SBDs prevent the operation of the securities markets or companies, such as a regional power outage, floods, terrorist attack or a wide scale regional disruption. In this scenario, VFM's response relies more heavily on market conditions and systemic risks associated with such a catastrophe.
- b) Approval and execution authority:
- VFM EXCO are responsible for approving this Plan, and the COO and IT Manager/ Representative are responsible for conducting an annual review.
- (i) The Plan is submitted to the VFM Board for the Board to assess the effectiveness of the Plan as a risk mitigation measure.
- (ii) VFM EXCO, along with designated senior management, have the delegated authority to execute any of VFM's strategies for business continuity under this Plan.

c) Plan location and access:

FM will maintain copies of this BCP plan together with the annual reviews, and the changes that have been made to it for inspection on the VFM SharePoint DR site.

4) Business Description

VFM is an authorized Financial Services Provider (FSP # 608) delivering asset management services to a substantial number of institutional clients. These services include management of:

- a) Equity funds
- b) Fixed interest and inflation-linked bond funds
- c) Balanced, Target Return, and Absolute Return funds
- d) Multi-Asset funds
- e) Derivatives
- f) International investments
- g) Collective Investment Scheme Portfolios

VFM is responsible for *inter alia* placing and executing orders with intermediaries, confirming client fund structures, creating client reports, calculating fund performances, and liaising with clients. The back-office client administration function is outsourced to Maitland and Curo, who have their own Business Continuity Plans. VFM's IT support function is outsourced to iSquared who is an integral structure and resource in VFM's Disaster Recovery Plan (DRP).

5) Office Location

VFM operates from its premises at the following location:

Cape Town : 1st Floor, 5 Cavendish Street, Claremont
 Telephone : 27-21-670-4900/1
 Fax : 27-21-683-5788

VFM's parent company, the Vunani Group, operates from 2 premises:

Cape Town : 14th Floor, 2 Long Street, Cape Town
 Telephone : 27-21-481-6200
 Fax : 27-21-422-2823

Johannesburg : Vunani House, Vunani House, Vunani Office Park, 151 Katherine Street,
Sandown, Sandton
Telephone : 27-11-263-9500
Fax : 27-11-784-3095

6) Alternative Physical Location of Employees

In the event of an SBD where VFM's office infrastructure becomes unavailable, VFM staff will work from home.

As a result of the Covid-19 pandemic, working from home has been tried and tested and has become part of the VFM culture. (Post-pandemic all staff will be required to regularly connect to the company's data center via VPN.)

All employees will be notified telephonically and / or by e-mail of the status of the SBD daily including the plan to return the business to a normal footing.

7) Client Access to Funds

VFM does not maintain custody of client assets (scrip) but will continue to facilitate the movement of cash into and out of bank accounts. Clients can continue to send notification instructions to cashflows@vunanifm.co.za and will be notified of the change in physical address.

8) Data Back-up and Recovery

Electronic data back-up and recovery forms part of the SLA with iSquared (see separate document).

9) Financial and Operational Assessments

a) Operational Risk

In the event of an SBD, VFM will immediately identify by what means it can communicate with its employees, clients, critical business constituents, critical banks, critical counterparties, and regulators. Although the severity of an SBD may affect the available means of alternative

communication, the communication options VFM will employ will include the telephone, cellphone, e-mail and VFM's Web site.

The VFM data center (currently located in our server room) is replicated to iSquared DR site three times a day. This replicated site forms VFM's secondary data center. VFM email is completely cloud based (by making use of Exchange Online and Microsoft 365) and will not be affected in the event of a physical disaster at our primary data center. VFM also makes use of the services of MIMECAST where all e-mail communication is stored on MIMECAST servers and is available at any time from any location. In addition to replicating our server stack to the iSquared DR data center, essential VFM data is also archived to Mimecast's cloud-based archiving service providing a further level of redundancy in our backup strategy.

VFM's paper records are stored in accordance with regulatory requirements.

b) Financial and Credit Risk

In the event of an SBD, VFM will evaluate its ability to continue to fund its operations and remain in capital compliance. VFM will contact the critical banks and shareholders to appraise them of the financial status if necessary. If VFM determines that it may be unable to meet its obligations to those counterparties or otherwise continue to fund its operations, VFM will request financing from its shareholders and in conjunction with the Board, may consider other credit sources to fulfill its obligations to its clients, in the event that shareholders are unable to fund the company. If VFM cannot remedy a capital deficiency, it will file appropriate notices with its regulators and immediately take all appropriate steps to mitigate the exposure.

10) Mission Critical Systems

These systems are all documented in the disaster recovery plan (DRP).

11) Alternate Communications between the Company and Clients, Employees and Regulators

a) Clients

VFM communicates with its clients via telephone, cellphone, e-mail, its website, courier, and personal visits. In the event of an SBD, VFM will use the quickest and most effective means available to communicate with the other party.

b) Employees

VFM communicates with its employees via telephone, cellphone, e-mail, Microsoft Teams and in person. In the event of an SBD, VFM will assess which means of communication are still available. A WhatsApp group has been set up so that senior management can reach all employees quickly during an SBD. The Crisis Management Team, represented by the COO, CIO, IT Manager/Representative and iSquared, has been established to make decisions about the firm's status and operation during any internal or external SBD.

c) Regulators

- The Financial Sector Conduct Authority (FSCA). VFM files reports with the FSCA via e-mail, and the FSCA website using their online submissions E-Services.
- The Financial Intelligence Centre (FIC). VFM files reports if required via the internet using the GoAML system.
- South African Reserve Bank (SARB). VFM files reports via the Reserve Bank website.
VFM will continue to file required reports using the communication means available to it.

12) Critical Business Constituents and Counterparties

a) Business constituents

VFM has contacted its critical business constituents (businesses with which VFM has an ongoing commercial relationship in support of its operating activities, such as vendors providing VFM with critical services), and determined the extent to which it can continue a business relationship considering the internal or external SBD. VFM will quickly establish alternative arrangements if a

business constituent can no longer provide the needed goods or services because of an SBD to them or the company.

b) Counterparties

VFM will contact its critical counterparties, such as brokers and Maitland, to determine how best to communicate and carry out required transactions in light of the internal or external SBD.

Current systems	SBD Event	Alternative means of communication
Bloomberg	x	Email or telephone
Cyrus	x	Emails can be sent with trades
IRESS Pro	x	Emails can be sent with trades
NX Manager	x	Trade templates can be used to send info to Maitland
Email	x	Telephone Brokers
Telephone	x	Cell phones can be used

13) Disclosure of Business Continuity Plan

VFM provides a copy of the BCP to its clients on request.

In the event of a disaster, the focus of the company will shift from the current structure and function of "business as usual" to the structure and function of an organization working towards survival and the resumption of business operations. In the Plan, VFM's Crisis Management actions are structured into time-phases. Each phase includes specific actions and roles and responsibilities for teams and/or individuals.

Each functional business unit has a Business Recovery Plan. A high degree of interaction among all teams is required to execute the Business Continuity Plan. VFM's goal in a disaster is the resumption and recovery of normal business operations and technology environments within recovery time objectives. Close coordination will be maintained between the Crisis Management Team and Executive Management and any other applicable recovery team throughout the resumption and recovery operations.

Technology driven operations can continue to run indefinitely provided that staff can access the data centers for general operational maintenance.

To mitigate the risk of operational outages, VFM has taken all reasonable precautions at its offices through UPS systems, building has its own generator and offsite replication. To ensure resilience and protection of its sensitive data, VFM has archived backups managed by a third-party vendor, Mimecast.

14) Updates and Annual Review

Telephone list to be used can be found on the VFM intranet.

VFM will update this plan whenever there is a material change to its operations, structure, business, or location or to that of its significant service providers Maitland or iSquared. In addition, VFM EXCO will review this BCP annually, to modify it for any changes in operations, structure and /or business. Any such changes or modifications will be approved in writing by the Chief Operating Officer, and the IT Manager / representative.